UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/377,064	08/19/1999	SHINICHI KAWAMURA	02860.2148	7317

22852 7590 07/03/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
SMITHERS, MATTHEWS	
ART UNIT	**PAPER NUMBER**
2134	8

DATE MAILED: 07/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/377,064	Applicant(s) KAWAMURA ET AL.	
	Examiner Matthew B Smithers	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 August 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5,7 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Priority

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

The information disclosure statements filed November 8, 1999 and March 23, 2001have been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Objections

Claim 17 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 17 presently depends from claim 15 and recites the limitation "data translation means" which is not found in claims 15 or claim 12.

Claim Rejections - 35 USC § 112

Claim 51 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9, 12- 51 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent U.S. patent 5,870,470 granted to Johnson et al.

Regarding claim 1, Johnson meets the claimed limitations as follows:

"An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking bits dependent: on a plaintext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from a ciphertext before the ciphertext is output." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 2, Johnson meets the claimed limitations as follows: "An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined;

mask patterns every time encryption is performed;

means for masking intermediate bit data within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from the intermediate bit data masked by said masking means." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 3, Johnson meets the claimed limitations as follows: "An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

data translation means for performing data translation to intermediate data within said apparatus;

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns

and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking an input to said data translation means with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from an output from said data translation means which is masked by said masking means." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 4, Johnson meets the claimed limitations as follows: "An apparatus according to claim 1, wherein said means for masking the bits dependent on the plaintext within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the ciphertext comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 5, Johnson meets the claimed limitations as follows: "An apparatus according to claim 2, wherein said means for masking the intermediate bit data within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 6, Johnson meets the claimed limitations as follows:

"An apparatus according to claim 3, wherein said data translation means, said means for masking the input to said data translation means with the selected mask patterns, and said means for removing the influence of the mask a from the masked output from said data translation means comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 7, Johnson meets the claimed limitations as follows:

"An apparatus according to claim 3, further comprising:

first storage means for storing, in the form of a table, said means for randomly selecting one pattern of each of the pairs ai,ai (where i is a positive integer not less than one) of one or the plurality of predetermined mask patterns and the mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed, said means for masking the input to said data translation means with the mask patterns ai, and said means for removing the influence of the masks ai from the masked output from said data translation means;

second storage means for storing, in the form of a table, said means for masking the input to said data translation means with mask patterns a, and said means for removing an influence of the masks a from the masked output from said data translation means; and

masked data translation means for randomly selecting one of said first and second storage means every time encryption is performed, and performing the processing by said data translation means for masked data." see column 3, lines 11-22.

Regarding claim 8, Johnson meets the claimed limitations as follows: "An apparatus according to claim 1, wherein the pair a, a of the mask patterns and the mask patterns obtained by bit inversion comprises a pair a, a of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns." see column 3, line 29 to column 4, line 9.

Regarding claim 9, Johnson meets the claimed limitations as follows: "An apparatus according to claim 1, wherein the pair a, a of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed." see column 3, line 29 to column 4, line 9.

Regarding claim 12, Johnson meets the claimed limitations as follows: "A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs ai, ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

means for masking bits dependent on a ciphertext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from a plaintext before the plaintext is output." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 13, Johnson meets the claimed limitations as follows:

"A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

means for masking intermediate bit data within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from the intermediate bit data masked by said masking means." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 14, Johnson meets the claimed limitations as follows:
"A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

data translation means for performing data translation to intermediate data within said apparatus;

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

means for masking an input to said data translation means with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from an output from said data translation means which is masked by said masking means." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 15, Johnson meets the claimed limitations as follows: "An apparatus according to claim 12, wherein said means for masking the bits dependent on the plaintext within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the ciphertext comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 16, Johnson meets the claimed limitations as follows: "An apparatus according to claim 13, wherein said means for masking the intermediate bit data within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus w, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 17, Johnson meets the claimed limitations as follows: "An apparatus according to claim 15, wherein said data translation means, said means for masking the input to said data translation means with the selected mask patterns, and said means for removing the influence of the mask a from the masked output from said data translation means comprise one of an exclusive OR, addition or subtraction

with respect to a modulus, and multiplication or division with respect to the modulus." see column 5, lines 1-16.

Regarding claim 18, Johnson meets the claimed limitations as follows: "An apparatus according to claim 14, further comprising:

first storage means for storing, in the form of a table, said means for randomly selecting one pattern of each of the pairs ai,ai (where i is a positive integer not less than one) of one or the plurality of predetermined mask patterns and the mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed, said means for masking the input to said data translation means with the mask patterns ai, and means for removing the influence of the masks ai from the asked output from said data translation means;

second storage means for storing, in the form of a table, means for masking the input to said data translation means with mask patterns a, and means for removing an influence of the masks a from the masked output from said data translation means; and

masked data translation means for randomly selecting one of said first and second storage means every time decryption is performed, and performing the processing by said data translation means for masked data." see column 3, lines 11-22.

Regarding claim 19, Johnson meets the claimed limitations as follows: "An apparatus according to claim 12, wherein the pair a, a of the mask patterns and the mask patterns obtained by bit inversion comprises a pair a,a of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns." see column 3, line 29 to column 4, line 9.

Regarding claim 20, Johnson meets the claimed limitations as follows: "An apparatus according to claim 13, wherein the pair ai,ai of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed." see column 3, line 29 to column 4, line 9.

Claims 23, 26, 30 and 31 are method claims that are substantially equivalent to apparatus claims 1, 4, 8 and 9, respectively. Therefore claims 23, 26, 30 and 31 are rejected by a similar rationale.

Claims 24 and 27 are method claims that are substantially equivalent to apparatus claims 2 and 5, respectively. Therefore claims 24 and 27 are rejected by a similar rationale.

Claims 25, 28 and 29 are method claim that is substantially equivalent to apparatus claims 3, 6 and 7, respectively. Therefore claims 25, 28 and 29 are rejected by a similar rationale.

Claims 34, 37, 41 and 42 are method claims that are substantially equivalent to apparatus claims 12, 15, 19 and 20, respectively. Therefore claims 34, 37, 41 and 42 are rejected by a similar rationale.

Claims 35 and 38 are method claims that are substantially equivalent to apparatus claims 13 and 16, respectively. Therefore claims 35 and 38 are rejected by a similar rationale.

Claims 36, 39 and 40 are method claim that is substantially equivalent to apparatus claims 14, 17 and 18, respectively. Therefore claims 36, 39 and 40 are rejected by a similar rationale.

Claim 45 is a computer-usable program storage medium claim that is substantially equivalent to apparatus claims 1. Therefore claim 45 is rejected by a similar rationale.

Regarding claim 46, Johnson meets the claimed limitations as follows: "An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs ai,ai (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking bits dependent on a key within said apparatus with the mask patterns selected by said selection means;

data translation means for converting intermediate data within said apparatus with the key; and means for removing an influence of the mask a from an output from said data translation means." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Regarding claim 47, Johnson meets the claimed limitations as follows: "An apparatus according to claim 46, wherein the pair a, a of the mask patterns and the mask patterns obtained by bit inversion comprises a pair a,a of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns." see column 3, line 29 to column 4, line 9.

Regarding claim 48, Johnson meets the claimed limitations as follows:

"An apparatus according to claim 46, wherein the pair a, a of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed." see column 3, line 29 to column 4, line 9.

Regarding claim 51, Johnson meets the claimed limitations as follows:

"An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs (ai, ai) (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every predetermined period of time;

means for masking bits dependent on a plaintext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from a ciphertext before the ciphertext is output." see Abstract; column 3, lines 11-22; column 3, line 29 to column 4, line 9; column 4, line 32 to column 5, line 16 and column 6, lines 44-59.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10, 11, 21, 22, 32, 33, 43, 44, 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 5,870,470 granted to Johnson et al and further in view of U.S. patent 6,031,911 granted to Adams et al.

Regarding claims 10, 11, 21, 22, 32, 33, 43, 44, 49 and 50, Johnson et al discloses everything claimed as applied above (see claims 1, 12, 23, 34 and 46), however Johnson fails to specifically teach the use of Hamming weights. Adams teaches S-boxes with Hamming weights as one of its ideal properties that can be used in a block cipher (see column 3, lines 9-39 and column 7, lines 6-22). It would have been obvious to one of ordinary skill in the at the time of the invention to combine Adams' practical design for S-boxes used in a block cipher with Johnson's apparatus for block ciphers in order to increase the security of block ciphers by decreasing the exploitability of an S-box [see Adams et al; column 3, lines 47-50 and column 7, lines 3-6].

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Elander et al (5,323,464) discloses commercial data masking in a communication system.

B. Begin et al (5,682,395) discloses an apparatus for correcting encoded data bits.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B. Smithers

Matthew B Smithers
Primary Examiner
Art Unit 2134

June 27, 2003